



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



020.201 Server Patch Management Policy





**Version 2.3
October 25, 2018**

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS IT Policies Team Charter
10/25/2018	2.3	Review Date	CHFS OATS Policy Charter Team
10/25/2018	2.3	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/25/2018		
CHFS Chief Information Security Officer (or designee)	10/25/2018		

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE	6
3	ROLES AND RESPONSIBILITIES	6
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	6
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
4	POLICY REQUIREMENTS	7
4.1	GENERAL SERVER PATCH MANAGEMENT	7
4.2	PATCH CYCLE STAGES	8
4.3	EMERGENCY/OFF-SCHEDULE PATCHES	8
5	POLICY MAINTENANCE RESPONSIBILITY	8
6	POLICY EXCEPTIONS	8
7	POLICY REVIEW CYCLE.....	8
8	POLICY REFERENCES	8

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

1 Policy Definitions

- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Emergency/Off-Schedule Patches:** Dates and times for any off-schedule Microsoft patch releases are approved and agreed upon between COT and the agency(s).
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **In-Scope Servers:** any server connected to a CHFS network managed by COT must follow the guidelines outlined above.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Production:** any server not in the Development, Test, or User Acceptance Testing/Training (UAT) environments. All servers are labeled (Development, Test, Production, etc.) in Information Technology Management Portal (ITMP). For example, File Servers are labeled as Production.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

- **System Center Operations Manager (SCOM):** is a cross-platform data center monitoring system for operating systems and hypervisors. It uses a single interface that shows state, health and performance information of computer systems
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through a server patch management policy. This document establishes the agency's Server Patch Management Policy, which helps manage patching cycles and provides guidelines for security best practices regarding patch management.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 General Server Patch Management

Operating system patches will be applied monthly by COT to CHFS servers, per their patch cycle. Emergency/off-schedule patches will be applied to all CHFS servers as soon as possible.

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

4.2 Patch Cycle Stages

COT will apply patches in four (4) stages:

- Stage 1- Patches will be applied to all Development (DEV) servers.
- Stage 2- Patches will be applied to all Test (TEST) servers.
- Stage 3- Patches will be applied to all User Acceptance Testing (UAT) and Training (TRN) servers.
- Stage 4- Patches will be applied to all Enterprise Production (PROD) servers.
- Stage 5- Patches will be applied to all System Center Operations Manager (SCOM) servers.
- Stage 6- Patches will be applied to all Production (PROD) servers.

COT will work with the agency for any downtime that may be required.

4.3 Emergency/Off-Schedule Patches

COT applies emergency/off-schedule patches as needed with notification to the CHFS OATS Patch Notification distribution list.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 010.103- Change Control Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessment Policy
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075

020.201 Server Patch Management Policy	Current Version: 2.3
020.200 Managerial Security	Review Date: 10/25/2018

- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information